802.1x と Web 認証 WLAN に関する LDAP 認証を使用した WLC の設定

内容

概要

このドキュメントでは、LDAPサーバを使用してクライアントをユーザデータベースとして認証するためにAireOS WLCを設定する手順について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- Microsoft Windows Server
- Active Directory

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアのバージョンに基づいています。

- Cisco WLC ソフトウェア 8.2.110.0
- Microsoft Windows Server 2012 R2

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

技術背景

- LDAP は、ディレクトリ サーバへのアクセスに使用されるプロトコルです。
- ディレクトリ サーバは、オブジェクト指向の階層型データベースです。
- オブジェクトは、組織単位(OU)、グループ、または既定のMicrosoftコンテナなどのコンテナにCN=Usersとして編成されます。
- このセットアップで最も難しい部分は、WLC で LDAP サーバ パラメータを正しく設定することです。

これらの概念に関する詳細については、『How to configure Wireless Lan Controller (WLC) for Lightweight Directory Access Protocol (LDAP) authentication（Lightweight Directory Access Protocol（LDAP）認証用のワイヤレス LAN コントローラ（WLC）の設定方法）』の「概要」の項を参照してください。

よく寄せられる質問（FAQ）

- LDAPサーバとのバインドに使用する必要があるユーザ名は何ですか。

LDAPサーバに対してバインドするには、匿名と認証済みの2つの方法があります（両方の方法の違いを理解するには、を参照してください）。

このバインドのユーザ名には他のユーザ名とパスワードを問い合わせることができる管理者権限が必要です。

- 認証済みの場合：バインドユーザ名はすべてのユーザと同じコンテナ内にありますか。

いいえ：パス全体を使用します。以下に、いくつかの例を示します。

CN=Administrator,CN=Domain Admins,CN=Users,DC=labm,DC=cisco,DC=com

Yes：ユーザ名のみを使用します。以下に、いくつかの例を示します。

Administrator

- 異なるコンテナにユーザが存在する場合はどうすればいいですか。関連するすべてのワイヤレス LDAP ユーザを同じコンテナに含める必要がありますか。

いいえ。必要なすべてのコンテナを含むベース DN を指定できます。

- WLCで検索する必要がある属性は何ですか。

WLCは、指定されたユーザ属性とオブジェクトタイプに一致します。

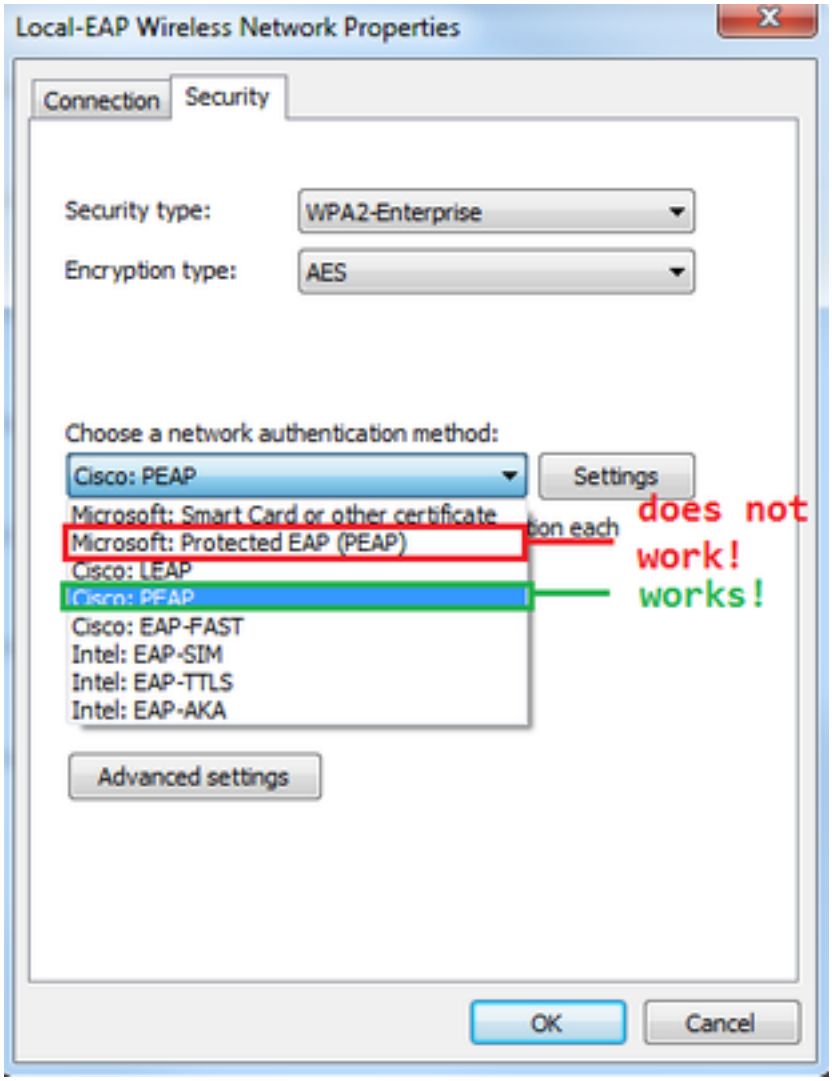
注：sAMAccountNameでは大文字と小文字が区別されますが、personでは区別されません

。したがって、sAMAccountName=RICARDOとsAMAccountName=ricardoは同じで機能しますが、samaccountname=RICARDOとsamaccountname=ricardoは機能しません。

- どのExtensible Authentication Protocol(EAP)方式を使用できますか。

EAP-FAST、PEAP-GTC、EAP-TLS のみです。Android、iOS、およびMacOSのデフォルトのサプリカントは、Protected Extensible Authentication Protocol(PEAP)で動作します。

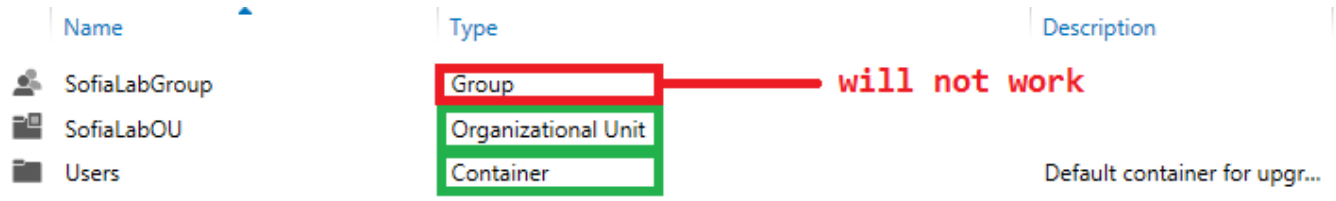
Windowsの場合は、図に示すように、Anyconnect Network Access Manager(NAM)またはCisco:PEAPを含むデフォルトのWindowsサプリカントを、サポートされているワイヤレスアダプタで使用する必要があります。



注:Cisco EAP Plug-ins for Windowsには、Cisco Bug ID CSCva09670の影響を受けるOpen Secure Socket Layer(OpenSSL 0.9.8k)のバージョンが含まれています。これ以降のリリースではWindows用EAPプラグインを発行する予定はなく、代わりにAnyConnectセキュアモビリティクライアントを使用することをお勧めします。

- WLCがユーザを検出できないのはなぜですか。

グループ内のユーザは認証できません。図に示すように、デフォルトコンテナ(CN)または組織単位(OU)内に配置する必要があります。



設定

802.1x認証またはWeb認証のいずれかでLDAPサーバを使用できるさまざまなシナリオがあります。

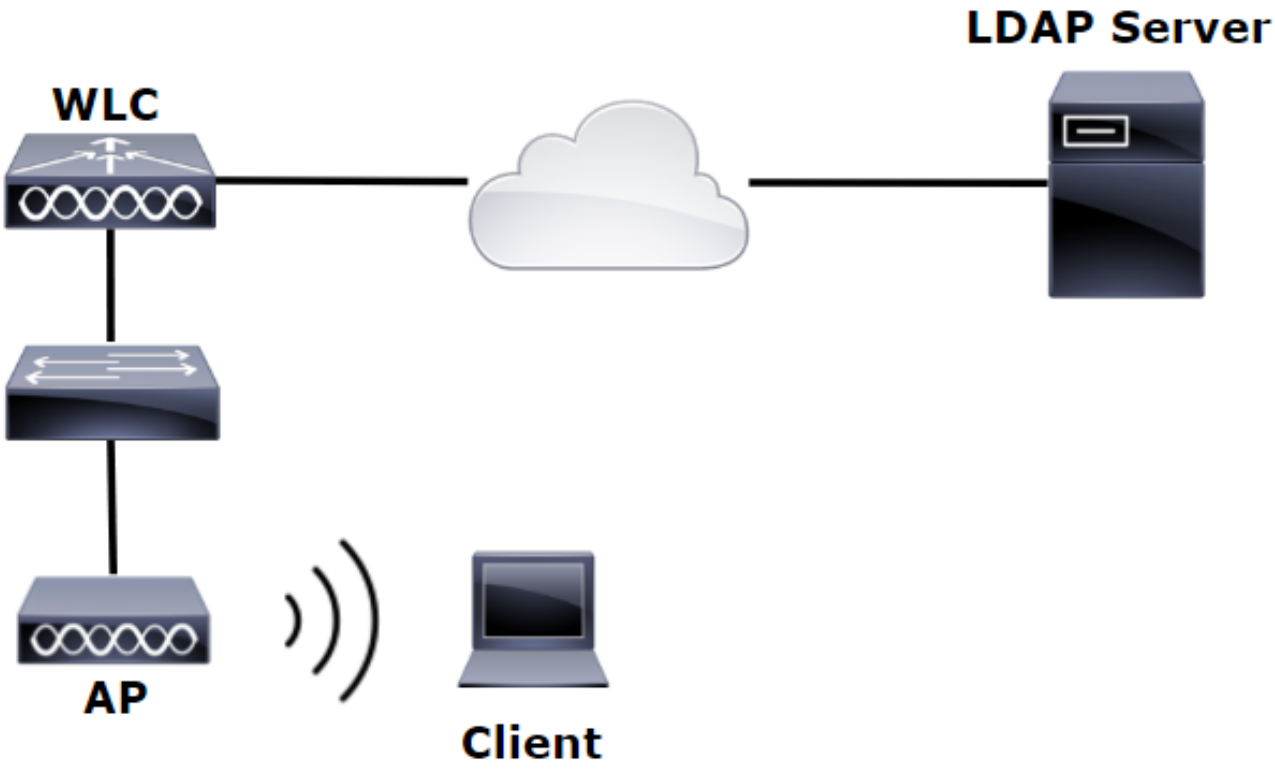
この手順では、OU=SofiaLabOU 内のユーザのみが認証されるようにする必要があります。

Label Distribution Protocol(LDP)ツールの使用方法、LDAPの設定およびトラブルシューティングについては、『WLC LDAPコンフィギュレーションガイド』を参照してください。

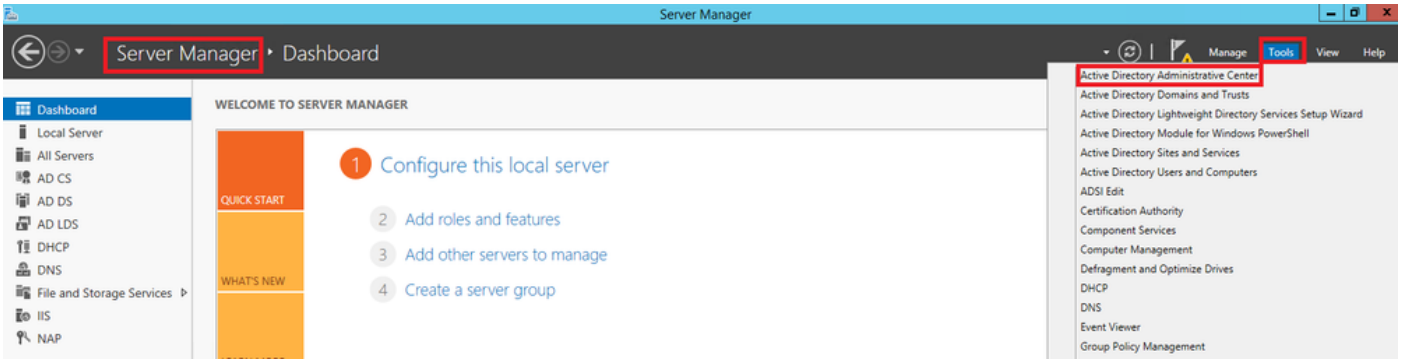
LDAPサーバを使用して802.1x経由でユーザを認証するWLANの作成

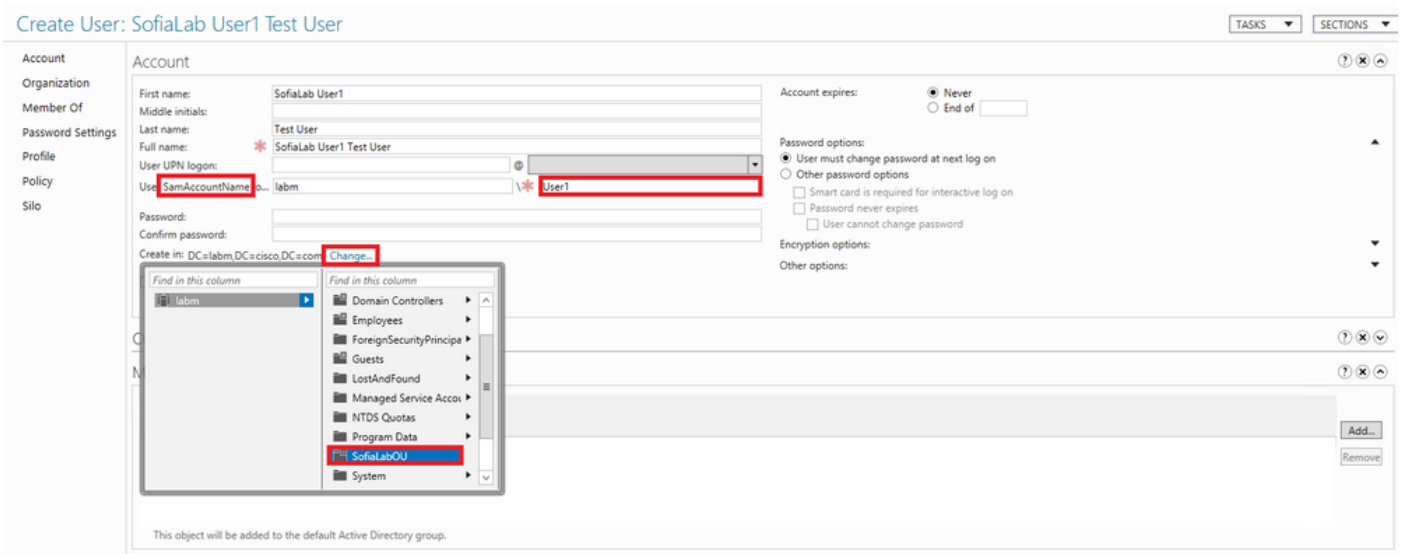
ネットワーク図

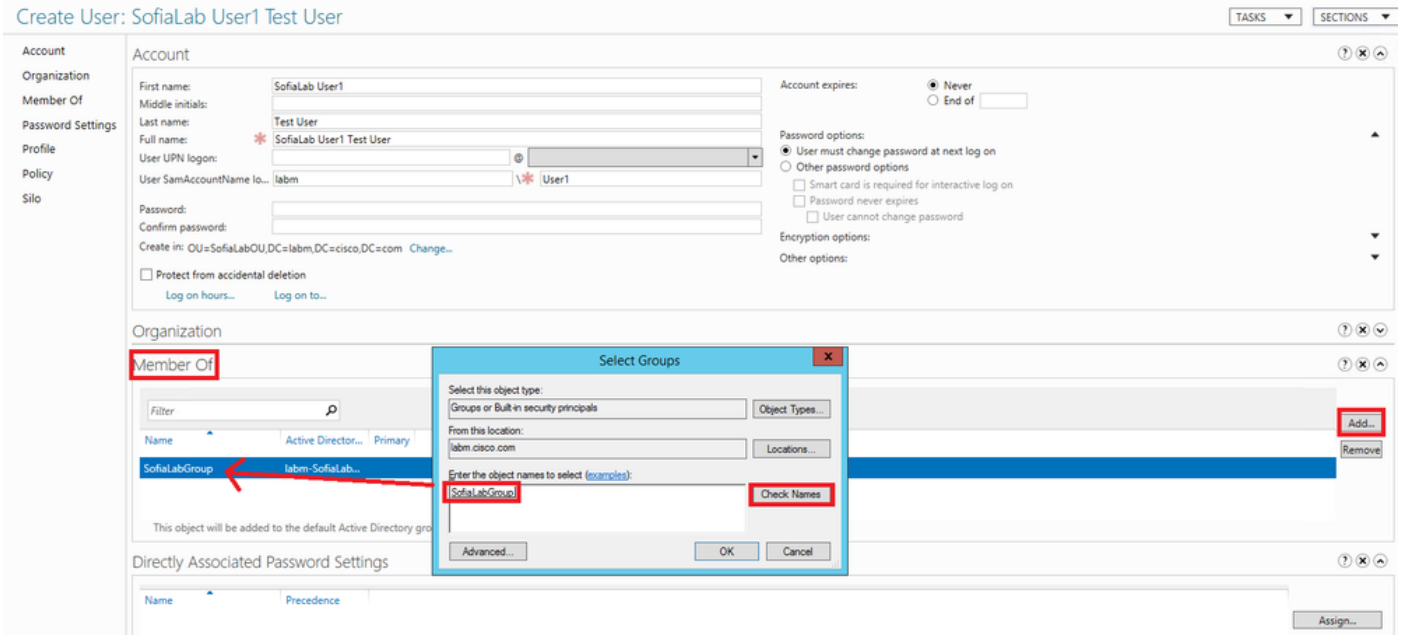
このシナリオでは、WLAN LDAP-dot1xはLDAPサーバを使用して、802.1xを使用してユーザを認証します。



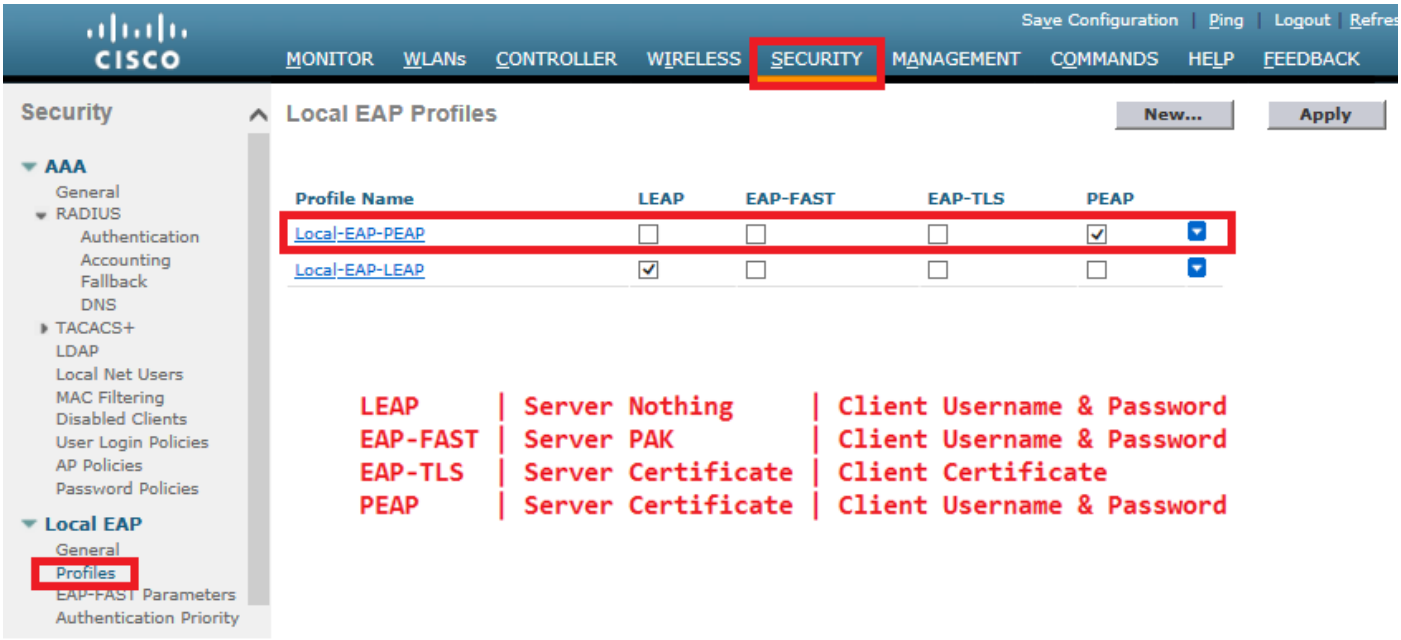
ステップ 1：SofiaLabOUとSofiaLabGroupのLDAPサーバメンバーにユーザ**User1**を作成します。





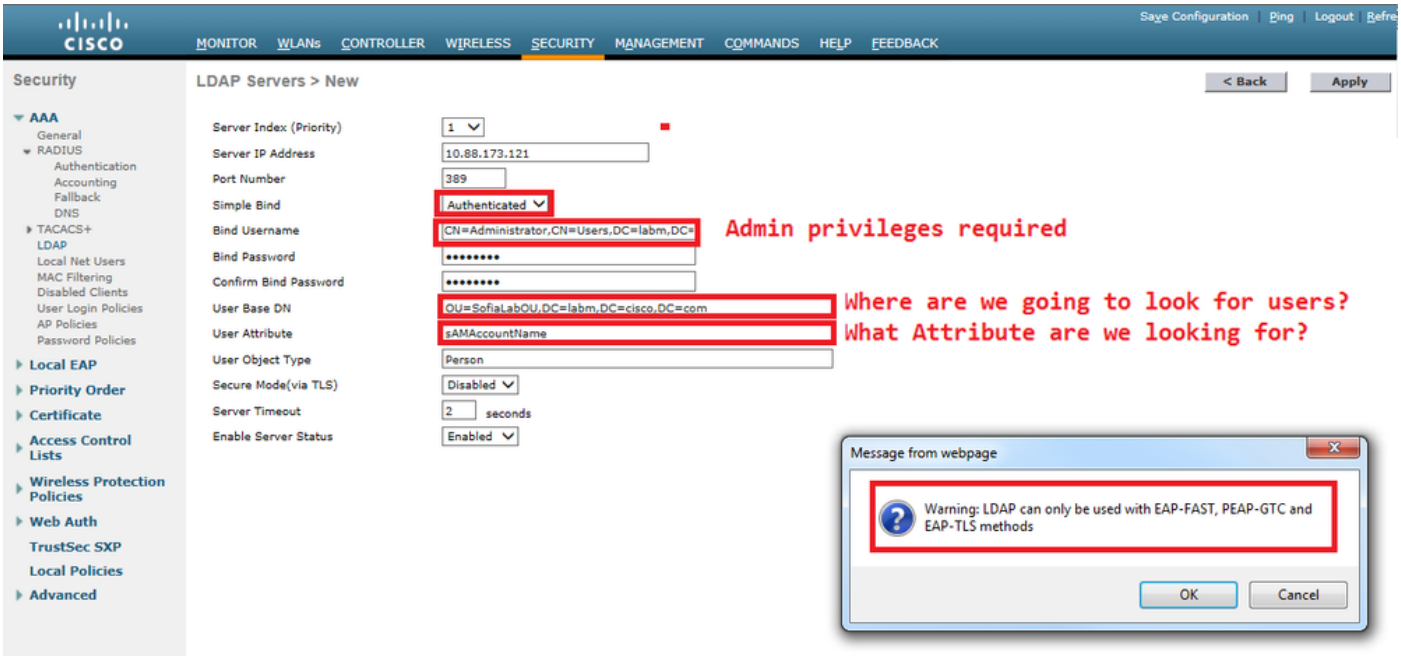


ステップ 2：目的のEAP方式でWLCにEAPプロファイルを作成します(PEAPを使用)。



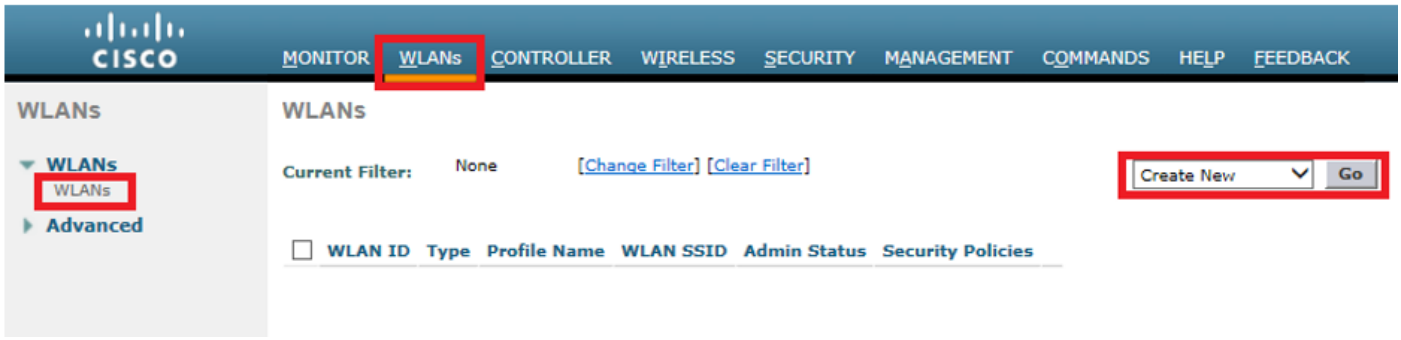
ステップ 3：WLCをLDAPサーバにバインドします。

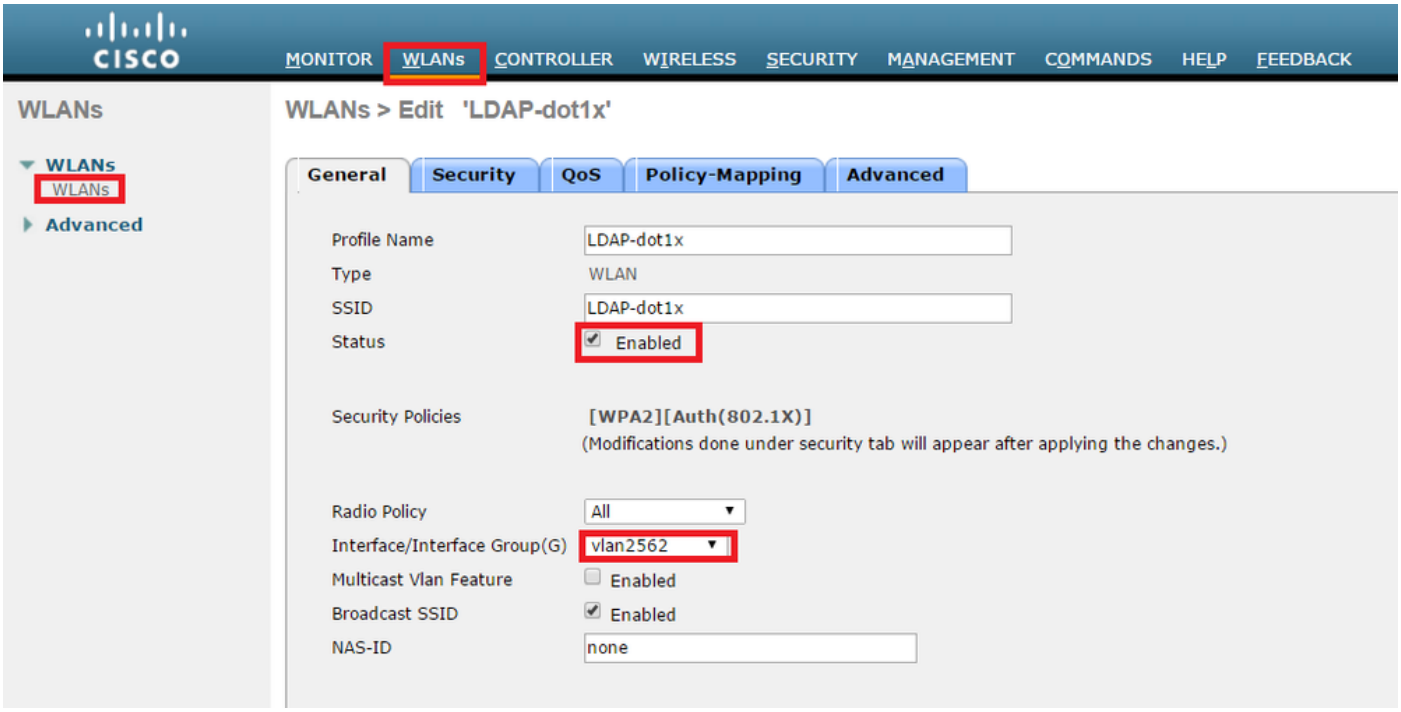
ヒント：バインドユーザ名がユーザベースDNにない場合は、次の図に示すように、Adminユーザへのパス全体を書き込む必要があります。それ以外の場合は、Administratorと入力します。



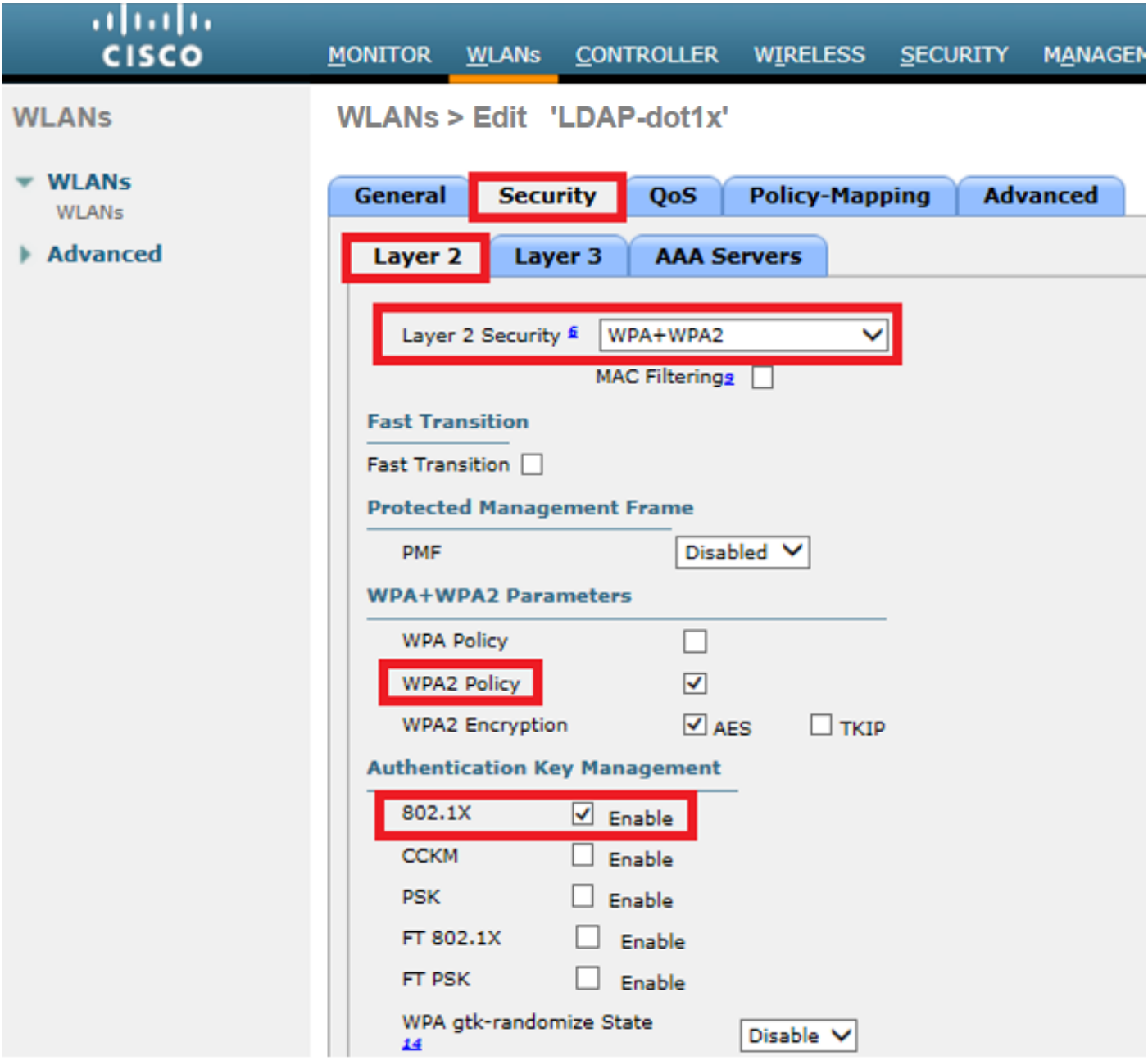
ステップ 4：[Authentication Order]を[Internal Users + LDAP or LDAP only]に設定します。

ステップ 5：LDAP-dot1x WLANを作成します。

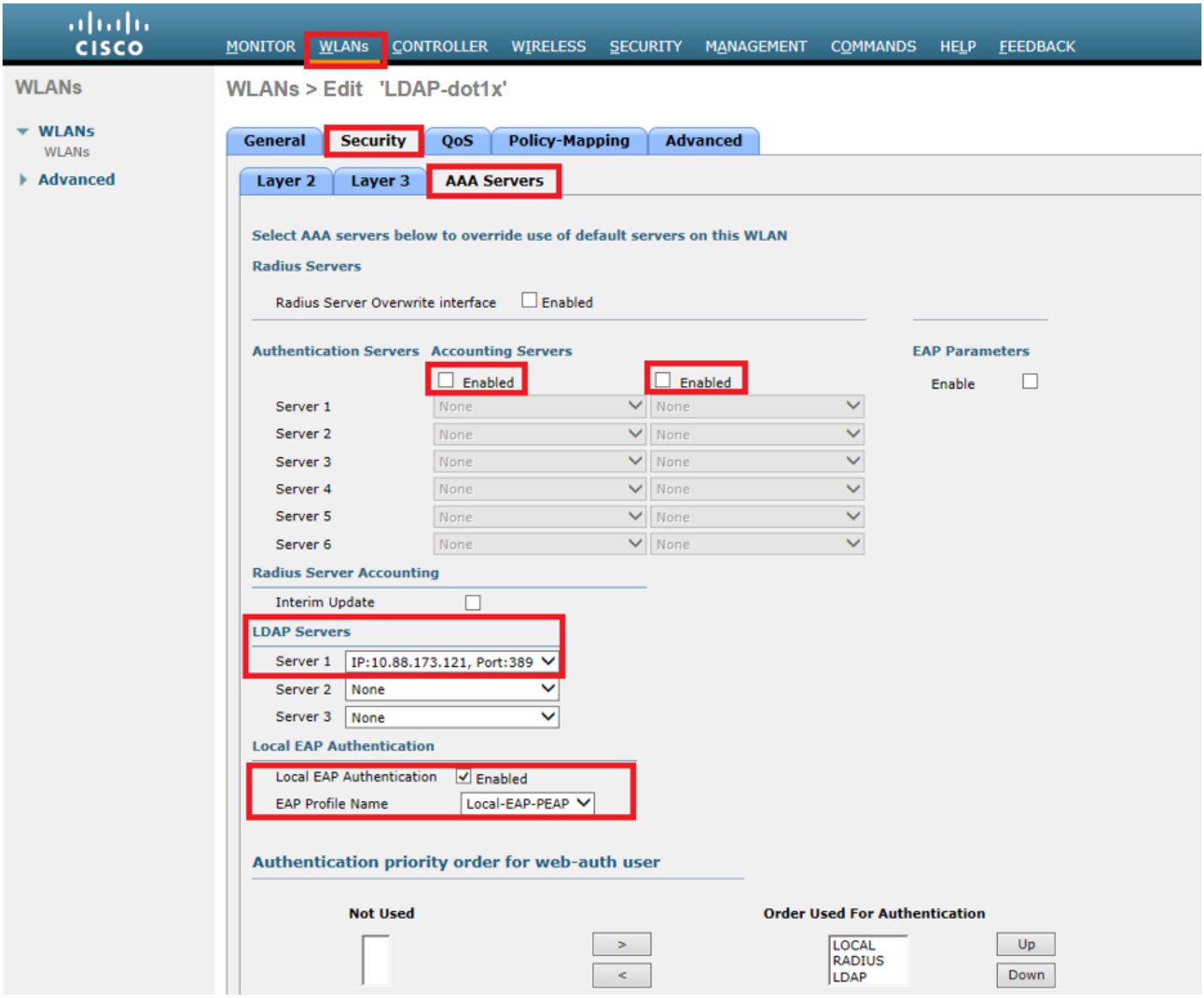




手順 6：L2セキュリティ方式をWPA2 + 802.1xに設定し、L3セキュリティをnoneに設定します。



手順 7：ローカルEAP認証を有効にし、[Authentication Servers]および[Accounting Servers]オプションが無効になっており、LDAPが有効になっていることを確認します。



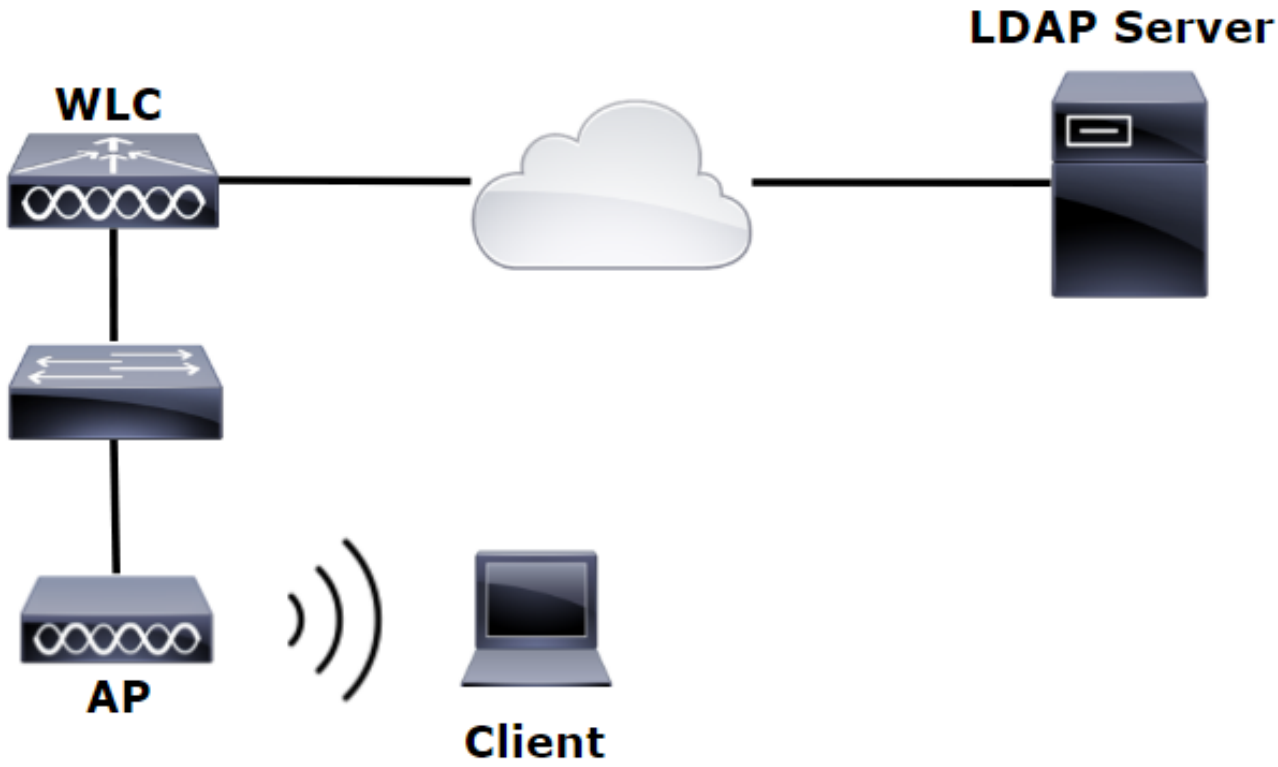
その他すべての設定は、デフォルトのままにすることができます。

> **注：**
> LDP ツールを使用して、設定パラメータを確認します。
> [Search Base] をグループ（SofiaLabGroup など）にすることはできません。
> Windowsマシンの場合は、サプリカントでMicrosoft:PEAPの代わりにPEAP-GTCまたはCisco:PEAPを使用する必要があります。Microsoft:PEAPは、デフォルトでMacOS/iOS/Androidで動作します。

内部WLC Webポータルを介してユーザを認証するLDAPサーバに依存するWLANの作成

ネットワーク図

このシナリオでは、WLAN LDAP-WebはLDAPサーバを使用して、内部WLC Webポータルでユーザを認証します。



前の例のステップ1 ~ 4が完了していることを確認します。それから、異なる WLAN 設定を指定します。

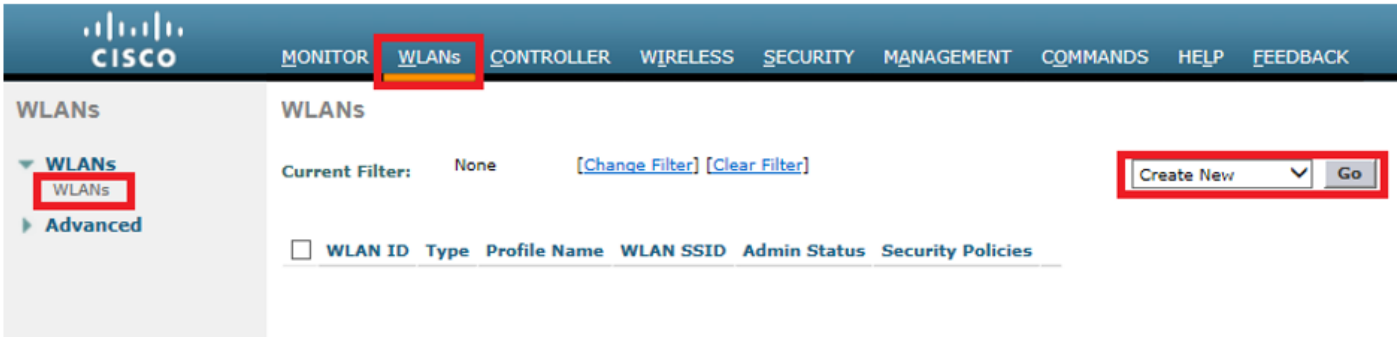
ステップ 1：OU SofiaLabOUとグループSofiaLabGroupのLDAPサーバメンバーにユーザ**User1**を作成します。

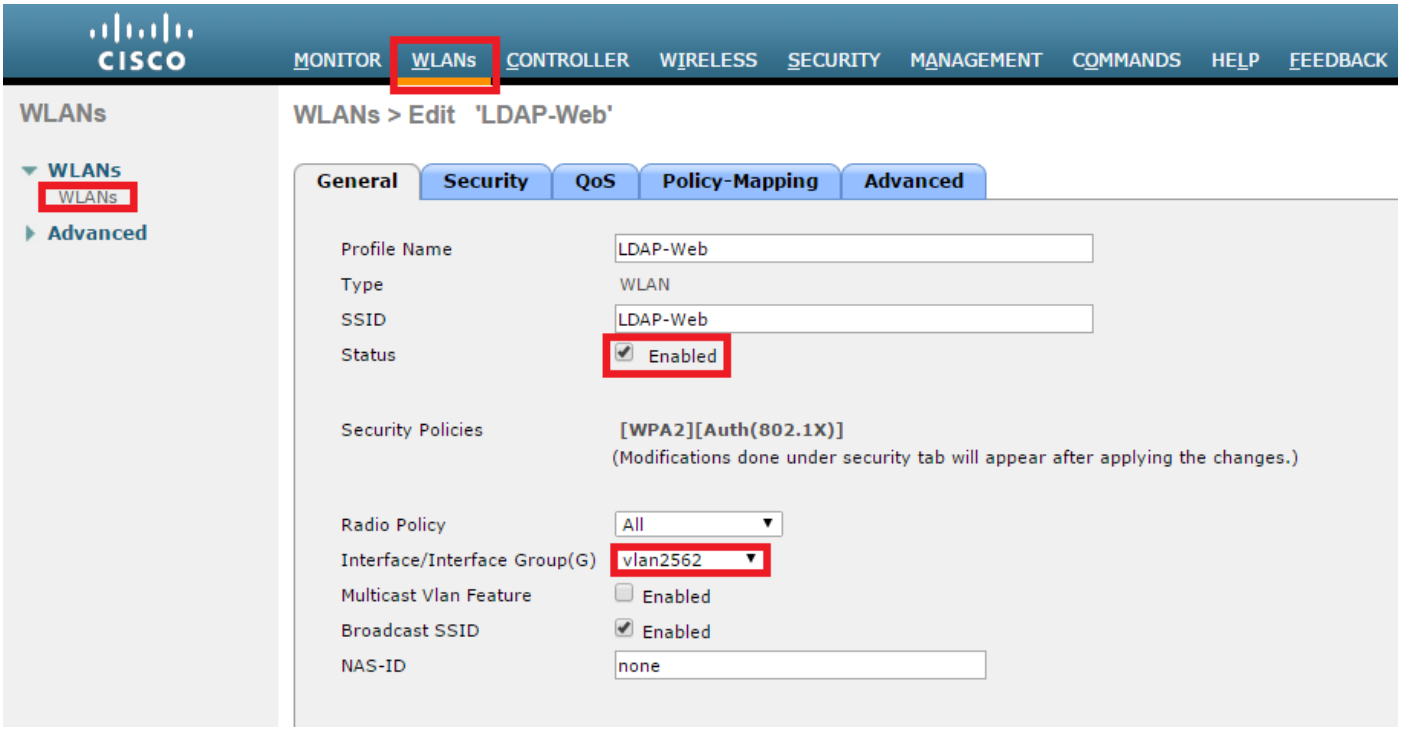
ステップ 2：目的のEAP方式でWLCにEAPプロファイルを作成します（PEAPを使用）。

ステップ 3：WLCをLDAPサーバにバインドします。

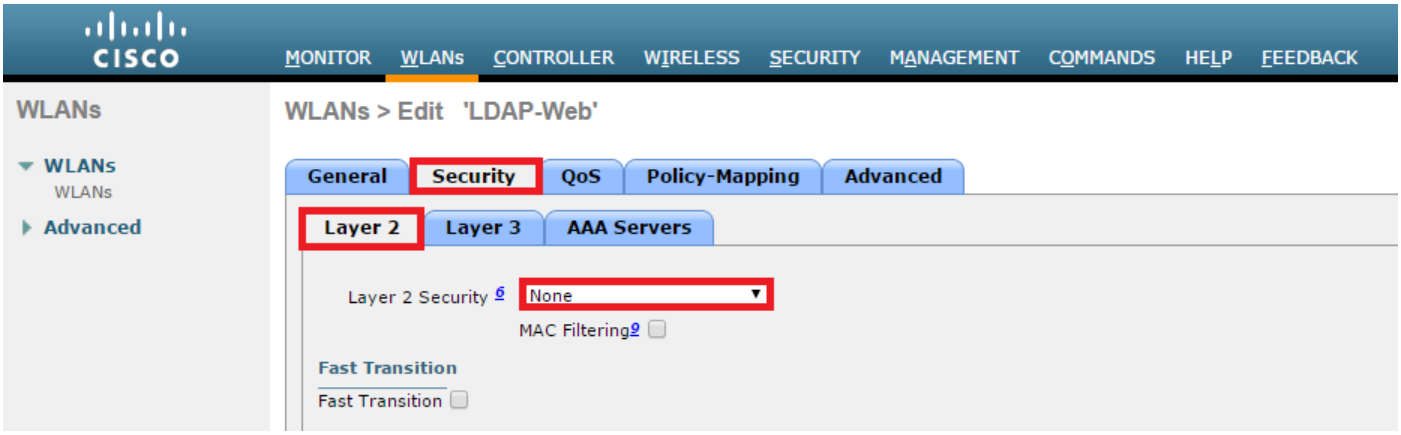
ステップ 4：[Authentication Order]を[Internal Users + LDAP]に設定します。

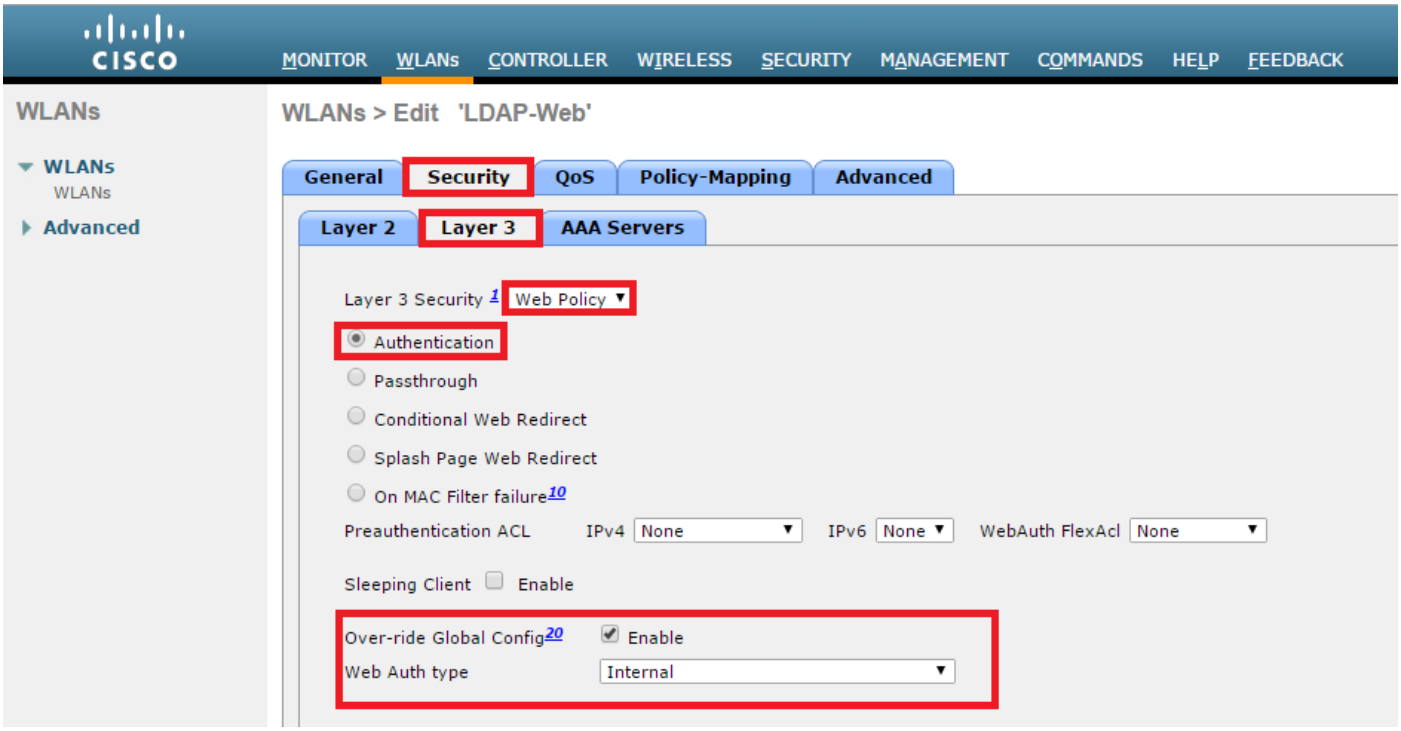
ステップ 5：図に示すように、LDAP-Web WLANを作成します。



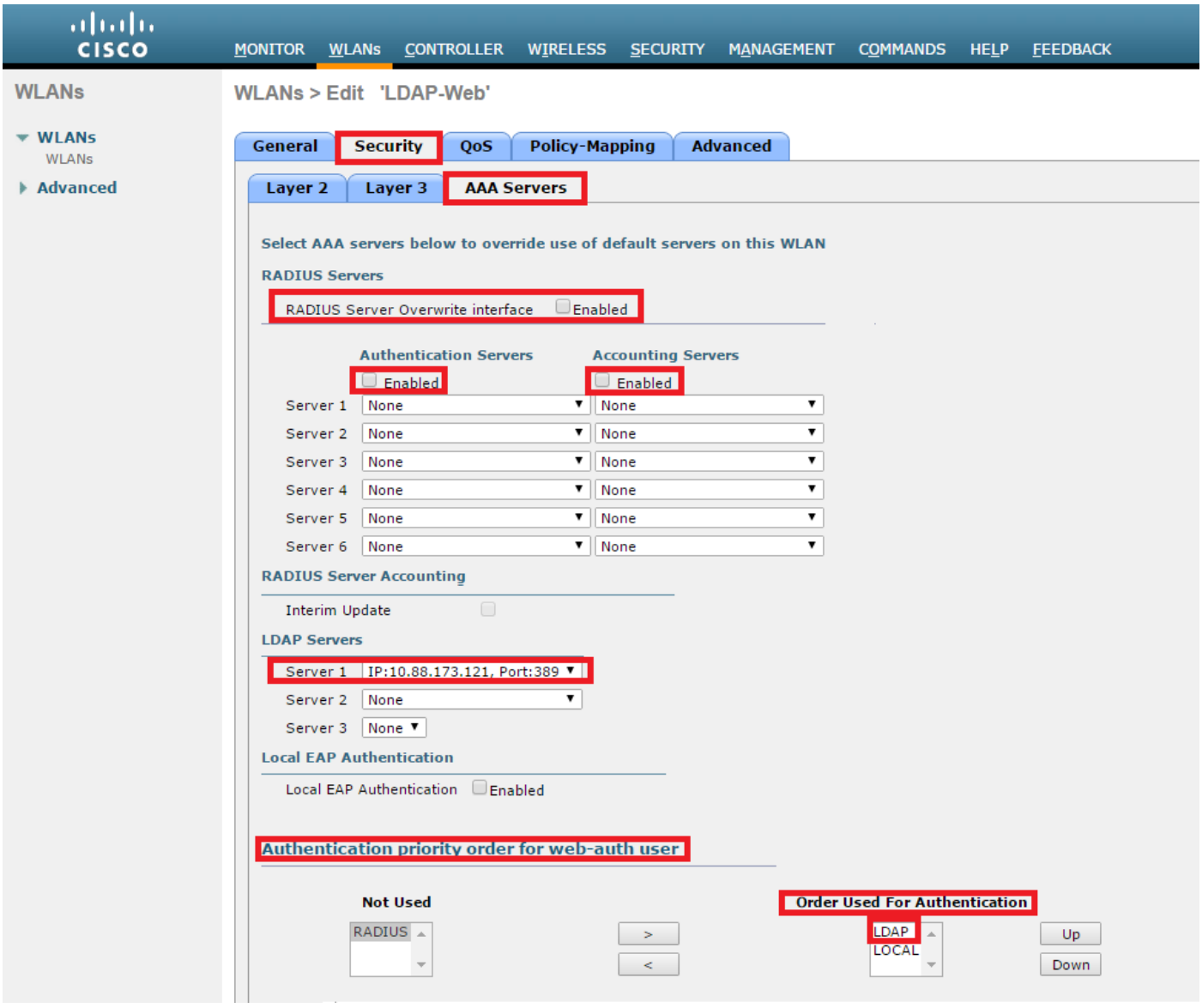


手順 6：[L2 Security]を[none]に、[L3 Security]を[Web Policy - Authentication]に設定します。図に示すように。





手順 7： Web認証の認証の優先順位をLDAPを使用するように設定し、[Authentication Servers]および[Accounting Servers]オプションが無効になっていることを確認します。

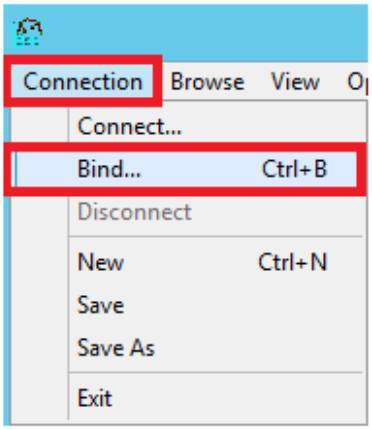


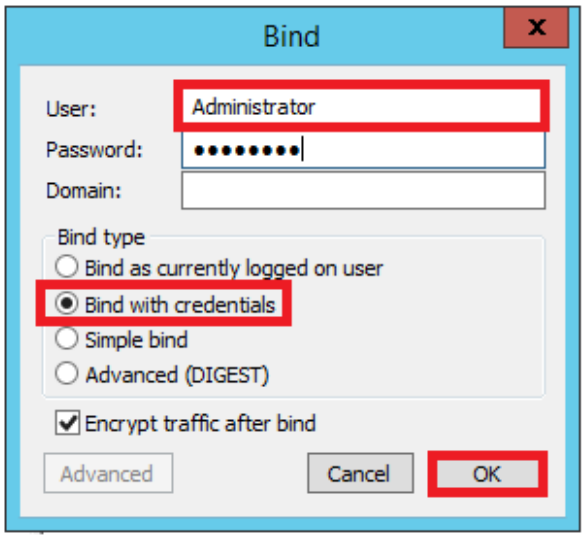
その他すべての設定は、デフォルトのままにすることができます。

LDAP ツールによる LDAP の設定とトラブルシューティング

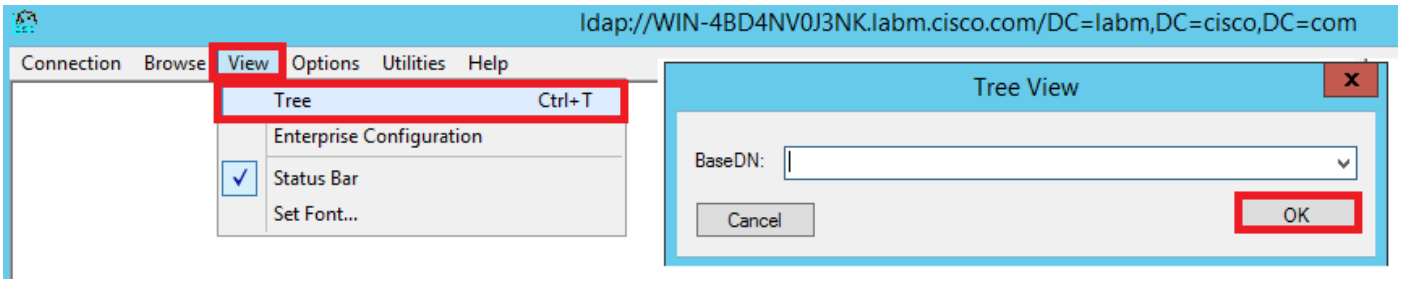
ステップ 1：LDAPサーバまたは接続されているホストのいずれかでLDPツールを開きます(サーバに対してポートTCP 389を許可する必要があります)。

ステップ 2： [Connection] > [Bind] に移動し、管理者ユーザでログインして、[Bind with credentials] オプションボタンを選択します。

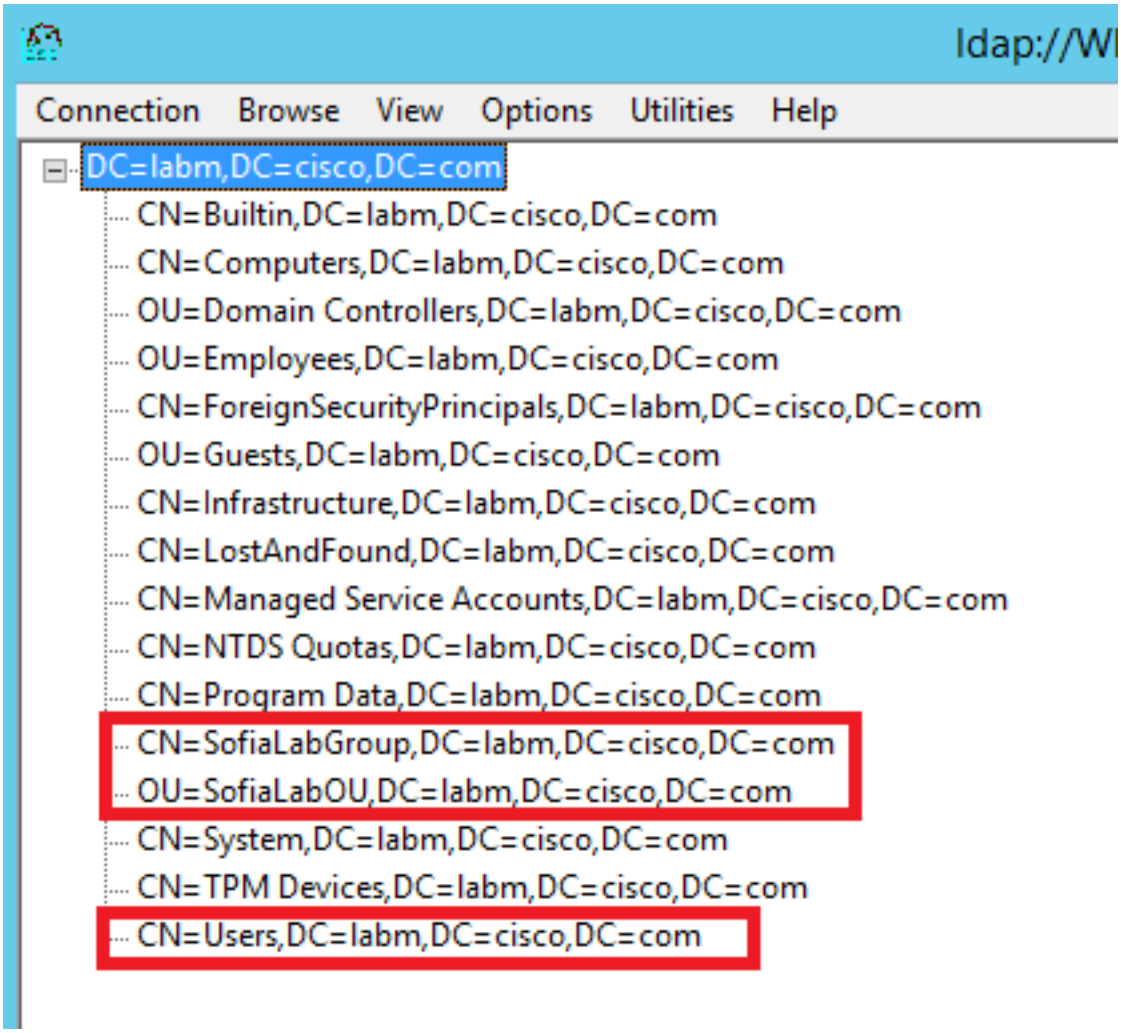




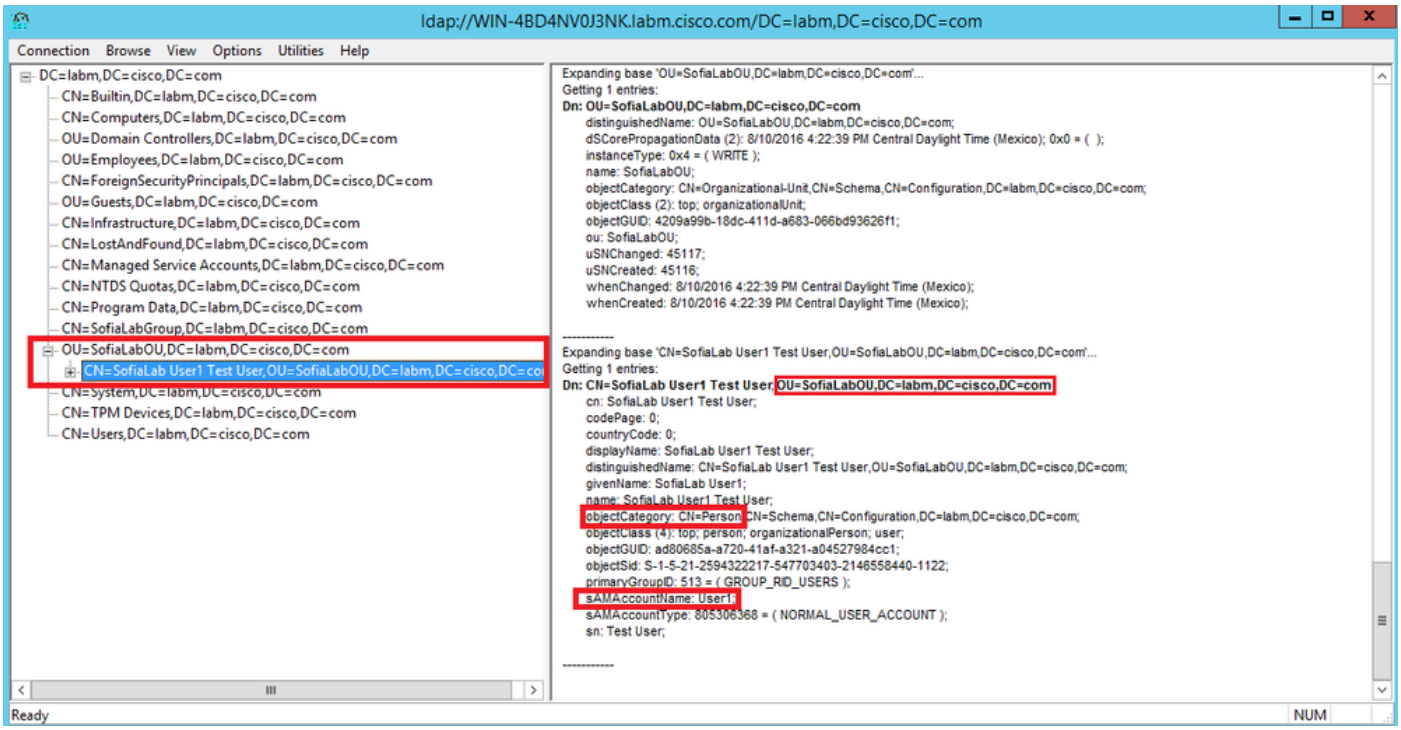
ステップ 3：[View] > [Tree] に移動し、ベースDNで[OK] を選択します。



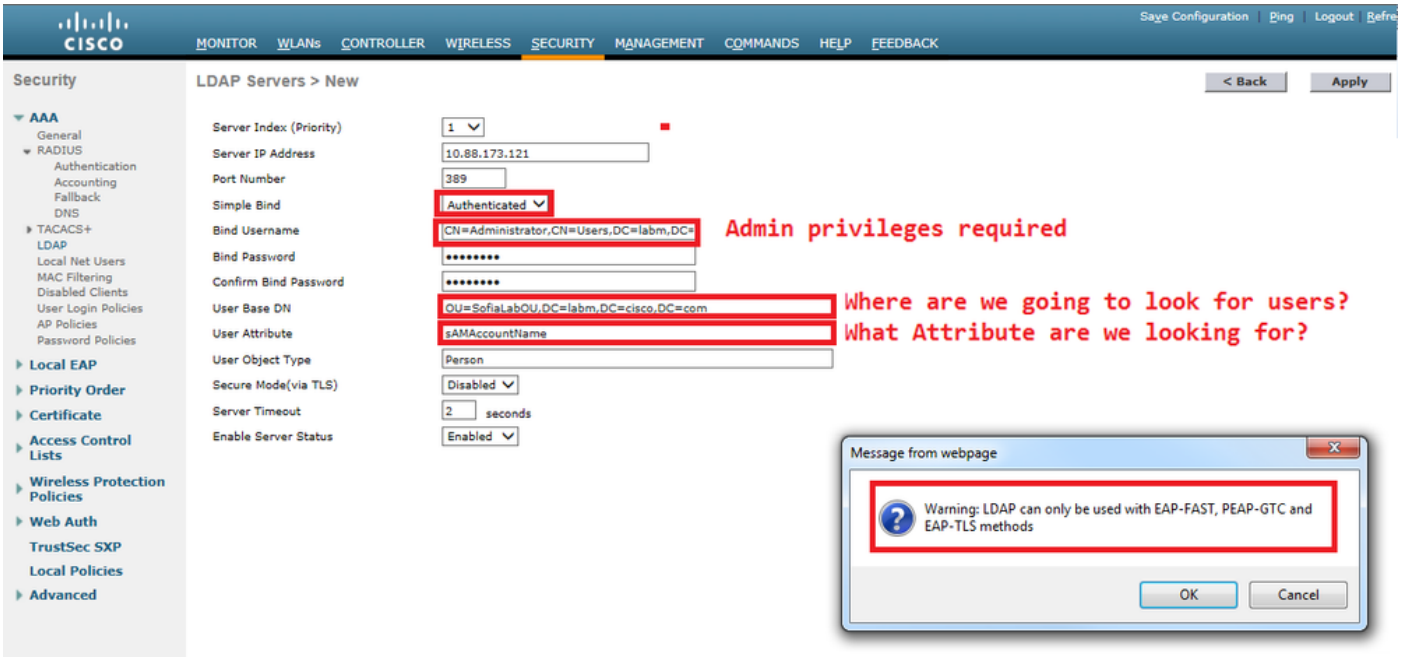
ステップ 4：ツリーを展開して構造を表示し、検索ベースDNを探します。グループ以外のいずれかのコンテナ タイプである可能性があることを考慮してください。ドメイン全体、特定の OU、または CN=Users などの CN である可能性があります。



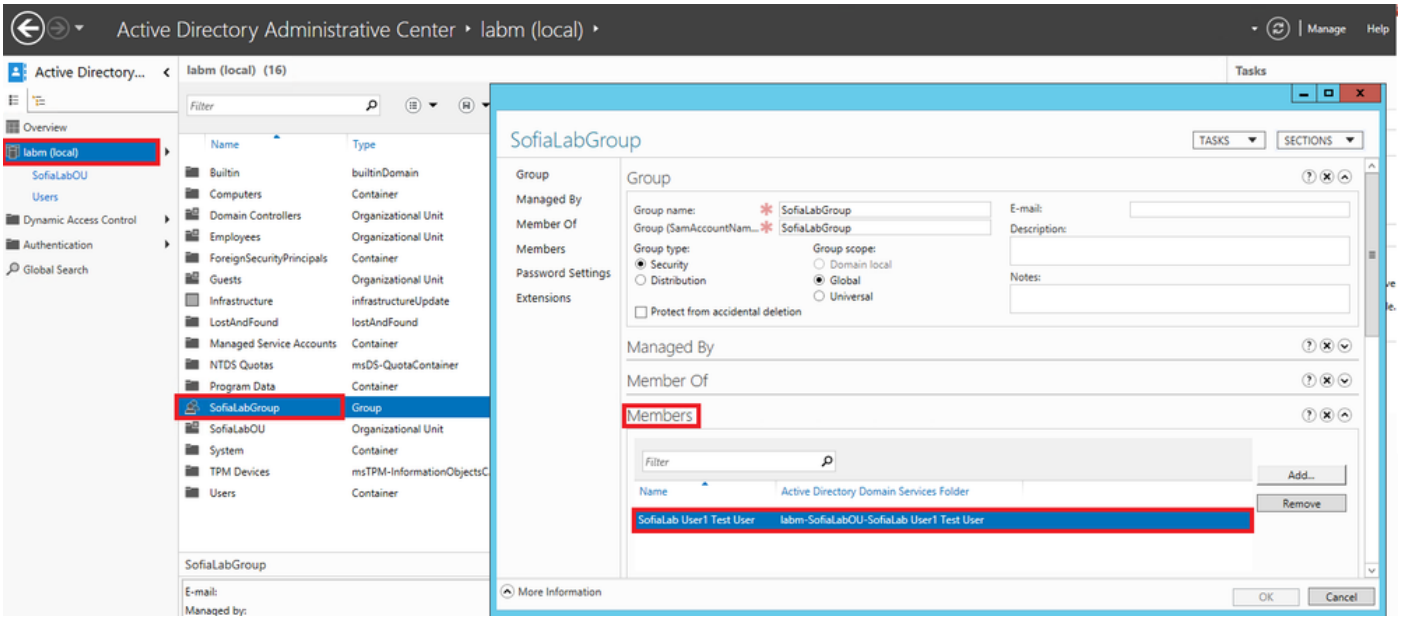
ステップ 5：SofiaLabOUを展開して、その中に存在するユーザを確認します。前に作成した User1 が含まれています。



手順 6：LDAPの設定に必要なすべてのこと。



手順 7：SofiaLabGroupなどのグループは検索DNとして使用できません。グループを展開し、そのグループ内のユーザを探します。ここで、先に作成したUser1がを参照してください。



User1 はありますが、それを LDP が見つけられませんでした。これは、WLCも同様に検索を実行できないことを意味し、グループが検索ベースDNとしてサポートされていない理由です。

確認

ここでは、設定が正常に機能しているかどうかを確認します。

```
(cisco-controller) >show ldap summary


Idx Server Address Port Enabled Secure
--- ---------------------- ------ ------- ------
1 10.88.173.121 389 Yes No
```

```
(cisco-controller) >show ldap 1

Server Index..................................... 1
Address.......................................... 10.88.173.121
Port............................................. 389
Server State..................................... Enabled
User DN.......................................... OU=SofiaLabOU,DC=labm,DC=cisco,DC=com
User Attribute................................... sAMAccountName
User Type........................................ Person
Retransmit Timeout............................... 2 seconds
Secure (via TLS)................................. Disabled
Bind Method ..................................... Authenticated
Bind Username.................................... CN=Administrator,CN=Domain
Admins,CN=Users,DC=labm,DC=cisco,DC=com
```

トラブルシュート

ここでは、設定のトラブルシューティングに使用できる情報を示します。

```
(cisco-controller) >debug client <MAC Address>

(cisco-controller) >debug aaa ldap enable

(cisco-controller) >show ldap statistics

Server Index..................................... 1
Server statistics:
Initialized OK................................... 0
Initialization failed............................ 0
Initialization retries........................... 0
Closed OK........................................ 0
Request statistics:
Received......................................... 0
Sent............................................. 0
OK............................................... 0
Success.......................................... 0
Authentication failed............................ 0
Server not found................................. 0
No received attributes........................... 0
No passed username............................... 0
Not connected to server.......................... 0
Internal error................................... 0
Retries.......................................... 0
```

関連情報

- 『LDAP - WLC 8.2 Configuration Guide（LDAP - WLC 8.2 設定ガイド）』
- 『How to configure Wireless Lan Controller (WLC) for Lightweight Directory Access Protocol (LDAP) authentication（Lightweight Directory Access Protocol（LDAP）認証用のワイヤレス LAN コントローラ（WLC）の設定方法）』（著者：Vinay Sharma）
- Web Authentication Using LDAP on Wireless LAN Controllers (WLCs) Configuration Example（ワイヤレス LAN コントローラ（WLC）での LDAP による Web 認証の設定例）（著者：Yahya Jaber および Ayman Alfares）
- テクニカル サポートとドキュメント – Cisco Systems

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。